了解随机无线加密流程

目录

简介

先决条件

- 要求
- 使用的组件

描述

步骤

实验室重现的详细信息

OWE FLOW

- 原始信标帧
- 隐藏的SSID信标
- 从客户端发送到OWE转换SSID的探测请求
- 从AP发送到客户端的探测响应
- 开放式身份验证
- 从客户端到AP的关联请求
- 从AP发送到客户端的关联响应
- 密钥交换
- L2身份验证成功
- IP学习状态
- 客户端处于运行状态
- 不支持OWE加密的客户端

快速过渡信息

PSK/dot1x不支持OWE

故障排除

- RA跟踪和EPC（嵌入式数据包捕获）
- AIR PCAP

漫游

简介

本文档介绍OWE转换流程及其在Catalyst 9800无线LAN控制器(WLC)上的工作方式。

先决条件

要求

Cisco 建议您了解以下主题：

- 如何配置9800 WLC（接入点[AP]）以实现基本操作
- 如何配置WLAN和策略配置文件。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- C9800-80、Cisco IOS® XE 17.12.4，还在Cisco IOS® XE 17.9.6中进行了测试
- AP型号：C9136I，已检查本地和灵活连接模式。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

描述

- OWE（机会性无线加密）是IEEE 802.11的扩展，为无线介质提供加密。基于OWE的身份验证的目的是避免AP和客户端之间的开放式非安全无线连接。
- OWE使用基于Diffie-Hellman算法的加密来设置无线加密。
- 使用OWE时，客户端和AP在访问过程中执行Diffie-Hellman密钥交换，并将生成的成对密钥与4次握手配合使用。
- 使用OWE可增强部署基于开放式或共享PSK的网络的无线网络安全性。

步骤

1. 配置一个不带任何加密/安全的开放式WLAN并启用广播。
2. 使用OWE安全设置配置另一个SSID，并在transition-mode-wlan-id中映射开放式WLAN ID号。禁用此OWE过渡SSID中的广播SSID选项。
3. 在OPEN WLAN“transition-mode-wlan-id”字段中映射OWE转换WLAN ID号。

实验室重现的详细信息

- 开放式SSID名称：未结欠款
- OWE转换SSID名称：OWE-Transition
- BSSID OF OPEN-OWE:40:ce:24:dd:2e:87
- OWE-Transition的BSSID:40:ce:24:dd:2e:8f

OWE FLOW

1. 可以广播开放式SSID的信标。您可以在AIR PCAP中通过其SSID名称看到它。
2. 我们还可以在AIR PCAP中看到名为“Wildcard”（通配符）而不是其自身SSID名称的启用隐藏安全的SSID。
3. 客户端收到开放SSID的信标帧后，如果它有或支持OWE，则它可开始向OWE过渡SSID（即启用安全功能的SSID而不是开放式SSID）发送探测请求。
4. OWE支持的客户端可以从转换SSID获取探测响应。

5. 客户端和AP之间可以进行OPEN身份验证。
6. 客户端可以向AP发送包含DH密钥交换详细信息的关联请求，并将生成的成对密钥用于4次握手。
7. AP可以发送关联响应。
8. AP和客户端设备之间可能会发生四次握手。
9. 密钥管理成功后，L2 PSK可以成功。
10. 客户端可以从DHCP、ARP等获取IP。
11. 客户端可以进入RUN状态。
12. 如果客户端设备不支持OWE，则它可以向OPEN SSID自身发送探测请求，并且可以直接获取IP，而不是进入RUN状态。

原始信标帧

- 此处，AIR PCAP显示SSID“OPEN-OWE”广播（信标帧）。 包含过渡SSID详细信息，称为“OWE-Transition”。

图1:开放式SSID的信标帧

隐藏的SSID信标

- 根据WLAN配置，此“OWE-Transition”SSID禁用“广播”，但是，您可以看到包含SSID名称“Wildcard”的AIR PCAP中的隐藏SSID信标。 但是，如果检查该数据包，它包含OWE-Transition详细信息。
- 使用此数据包（例如“40:ce:24:dd:2e:8f”）获取隐藏SSID的BSSID，并在数据包捕获中搜索它。
- 在此数据包中，它显示SSID“Missing”，并包含其转换SSID“OPEN-OWE”和BSSID“40:ce:24:dd:2e:87”。

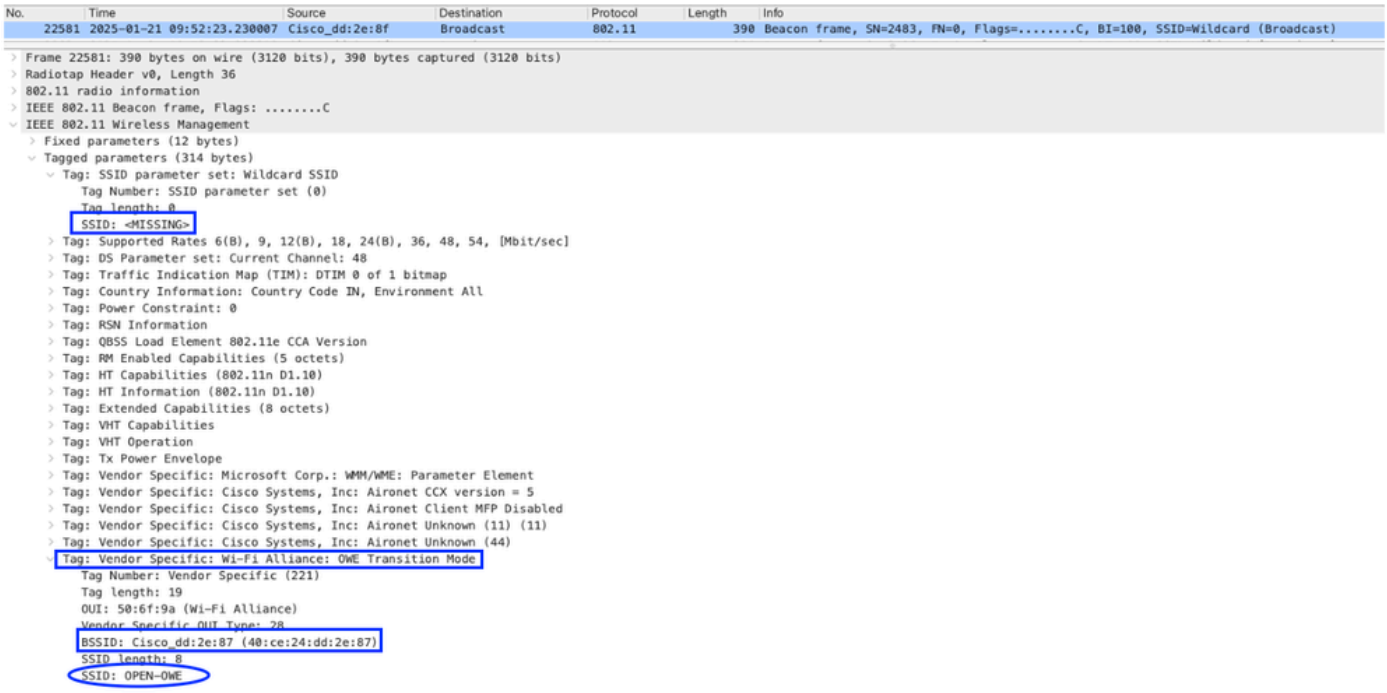

图2:隐藏SSID - OWE转换

从客户端发送到OWE转换SSID的探测请求

- 根据信标帧“OPEN-OWE” SSID，客户端知道需要连接的其他SSID详细信息，在本场景中为“OWE-Transition”。 如果客户端能够支持OWE加密，则它可以将探测请求发送到“OWE-Transition”SSID并获得响应。
- 探测请求发送到OWE-Transition BSSID "40:ce:24:dd:2e:8f"，并收到响应。在此探测响应数据包内，您还可以看到OPEN-OWE SSID详细信息。

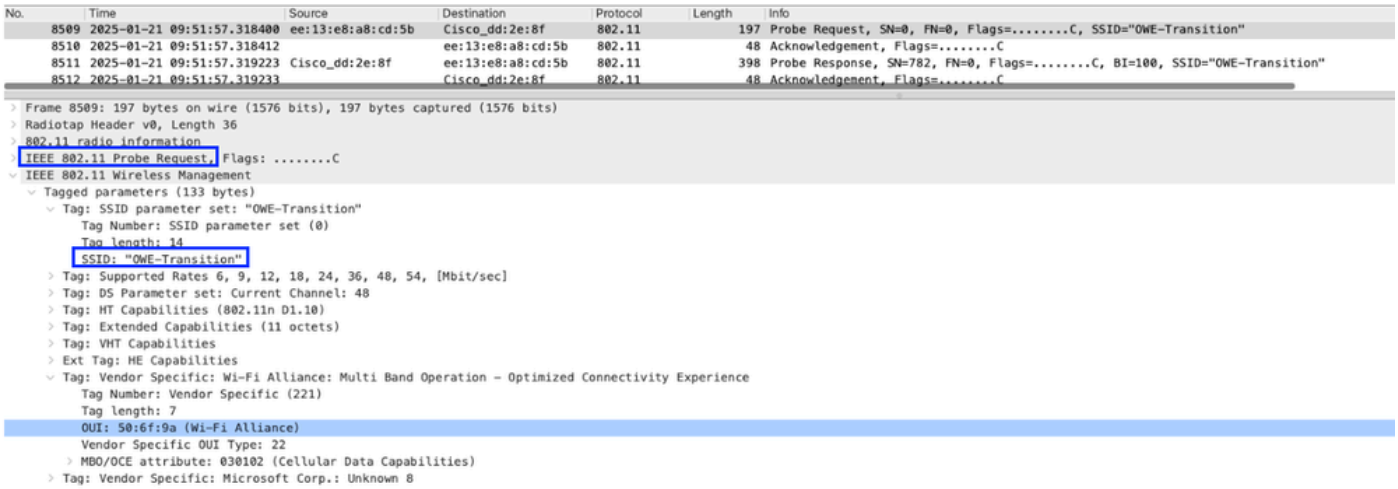

图3:探测请求

从AP发送到客户端的探测响应

- 客户端收到SSID“OWE-Transition”的探测响应，但是它在WiFi Alliance中有其原始SSID详细信息“OPEN-OWE”。

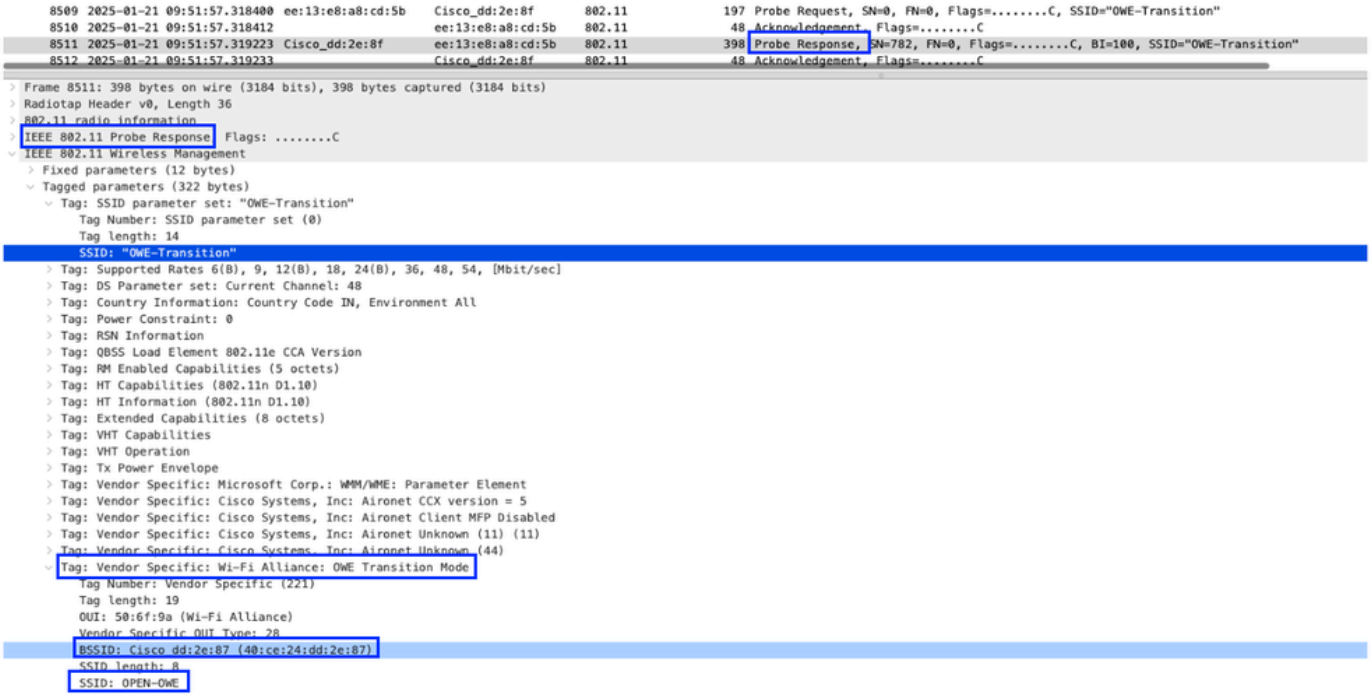

图4:探测响应

开放式身份验证

- 获得探测响应后，客户端和AP之间可能会进行OPEN身份验证，以在关联之前检查客户端的wifi详细信息/功能。

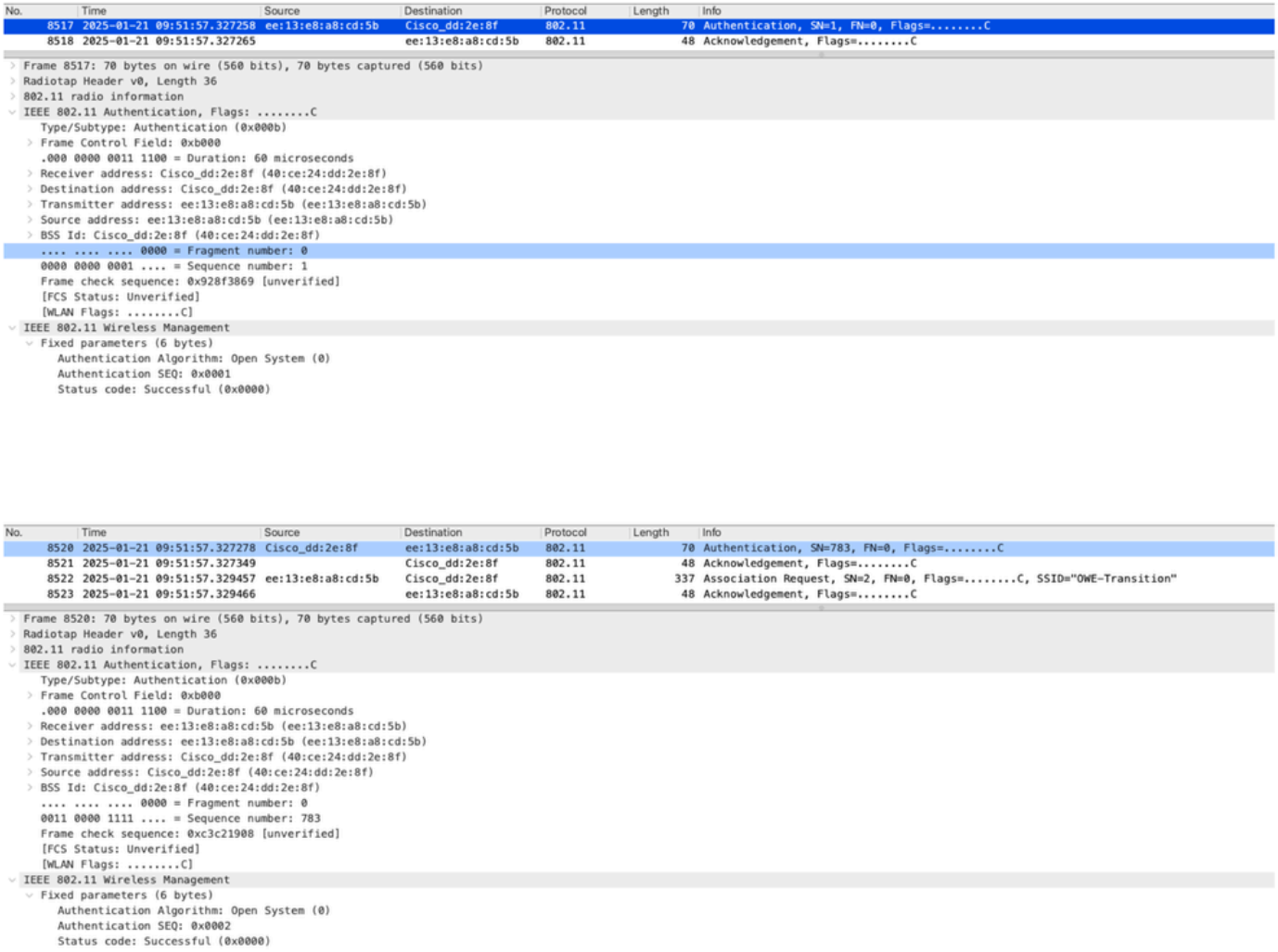

图5:探测成功后执行OPEN身份验证

从客户端到AP的关联请求

- 请注意，在此数据包中，客户端可以附加用于加密的Diffie-Hellman参数值。

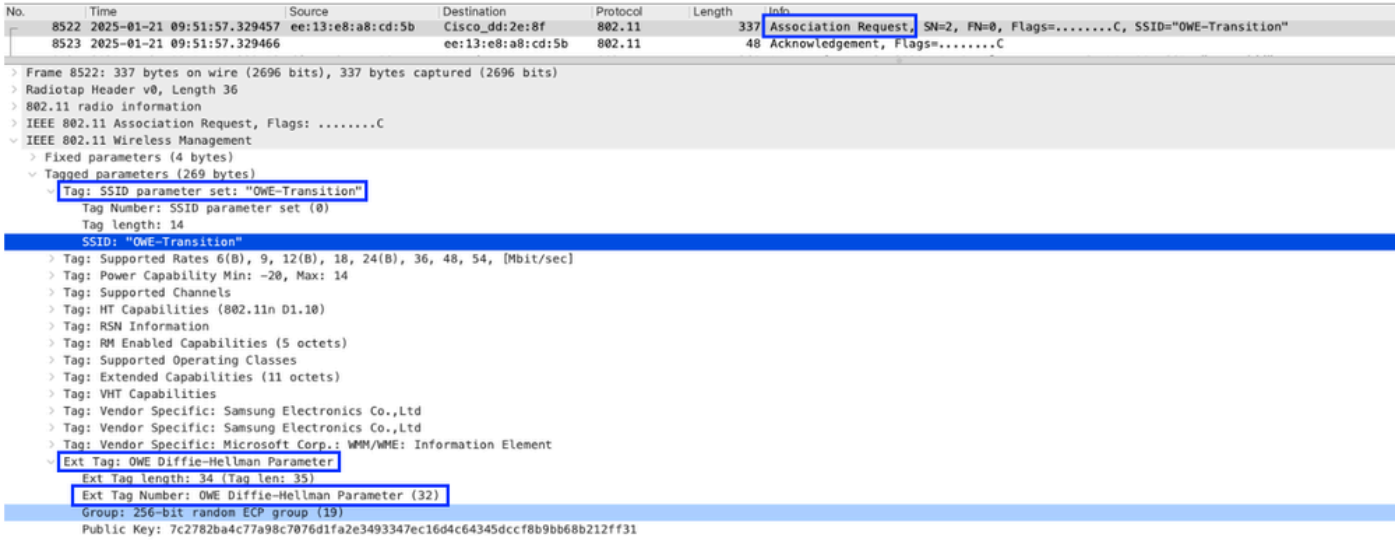

图6:关联请求

- 在RA跟踪中，您可以开始查看关联阶段的客户端日志，

```
2025/01/21 15:21:57.391071821 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (note): MAC: ee13.e8a8.cd5b  A
2025/01/21 15:21:57.391117645 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b
```

从AP发送到客户端的关联响应

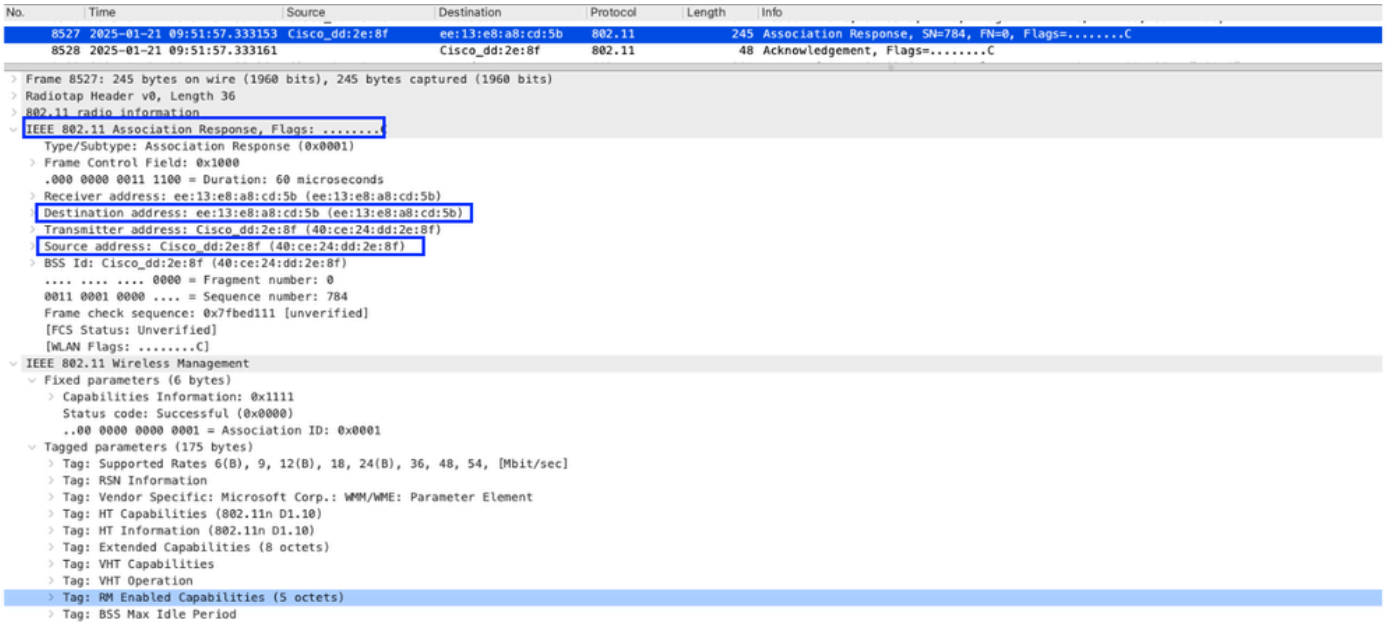

图7:关联响应

```
2025/01/21 15:21:57.391334260 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
2025/01/21 15:21:57.392296819 {wncd_x_R0-0}{1}: [dot11] [21675]: (note): MAC: ee13.e8a8.cd5b  Associati
```

密钥交换

AP和客户端设备之间可能会发生4次握手。

Key-1由AP发送

客户端发送的密钥2

Key-3由AP发送

Key-4由客户端发送

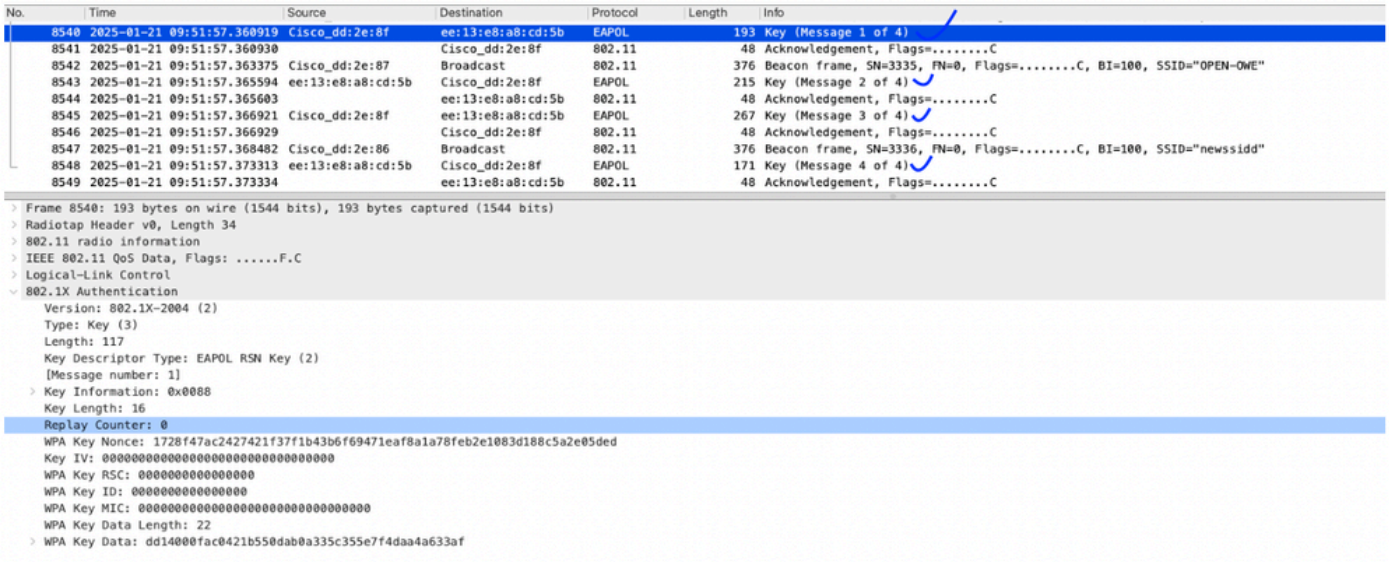

图8:4次握手

```
2025/01/21 15:21:57.392538716 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.392557538 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
2025/01/21 15:21:57.392640494 {wncd_x_R0-0}{1}: [client-auth] [21675]: (note): MAC: ee13.e8a8.cd5b  L2
2025/01/21 15:21:57.394830551 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b  Cli
2025/01/21 15:21:57.395171903 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b  Cli
2025/01/21 15:21:57.420590731 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b  Cli

2025/01/21 15:21:57.420706435 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.420775720 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.426548998 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.426725965 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.426727805 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.434078994 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.434099154 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (note): MAC: ee13.e8a8.cd5b
```

L2身份验证成功

```
2025/01/21 15:21:57.434111288 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.434250308 {wncd_x_R0-0}{1}: [client-auth] [21675]: (note): MAC: ee13.e8a8.cd5b  L2
2025/01/21 15:21:57.434286035 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b  Cli
2025/01/21 15:21:57.434308953 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b
```

IP学习状态

```
2025/01/21 15:21:57.434789679 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.436611026 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
2025/01/21 15:21:57.437239513 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
2025/01/21 15:21:57.437508189 {wncd_x_R0-0}{1}: [client-iplearn] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.534166453 {wncd_x_R0-0}{1}: [sisf-packet] [21675]: (info): TX: DHCPv4 from interfac
2025/01/21 15:21:57.535325325 {wncd_x_R0-0}{1}: [client-iplearn] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.535874658 {wncd_x_R0-0}{1}: [sisf-packet] [21675]: (info): TX: DHCPv4 from interfac
2025/01/21 15:21:57.536500021 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b
```

客户端处于运行状态

```
2025/01/21 15:21:57.537017277 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
```

不支持OWE加密的客户端

- 通过检查信标帧本身，客户端可以了解它们是否能够支持此加密方法。如果不受支持，则它只需发送探测请求到开放式SSID“OPEN-OWE”，并可执行正常的开放身份验证，获取IP地址，然后进入RUN状态。

```
2025/01/16 15:36:06.178370757 {wncd_x_R0-2}{1}: [client-orch-sm] [17332]: (note): MAC: d037.4587.8f35
2025/01/16 15:36:06.209288788 {wncd_x_R0-2}{1}: [dot11] [17332]: (note): MAC: d037.4587.8f35  Associati
2025/01/16 15:36:06.248651191 {wncd_x_R0-2}{1}: [client-auth] [17332]: (note): MAC: d037.4587.8f35  Ope
2025/01/16 15:36:06.248751507 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
2025/01/16 15:36:06.281808554 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
2025/01/16 15:36:06.303307756 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
2025/01/16 15:36:10.305041414 {wncd_x_R0-2}{1}: [client-iplearn] [17332]: (note): MAC: d037.4587.8f35
2025/01/16 15:36:10.305777492 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
```

快速过渡信息

- 我们只能在OPEN身份验证或Webauth(CWA/LWA/EWA)中配置OWE。
- OWE转换不支持FT。
- 如果启用FT，则会收到此错误消息，

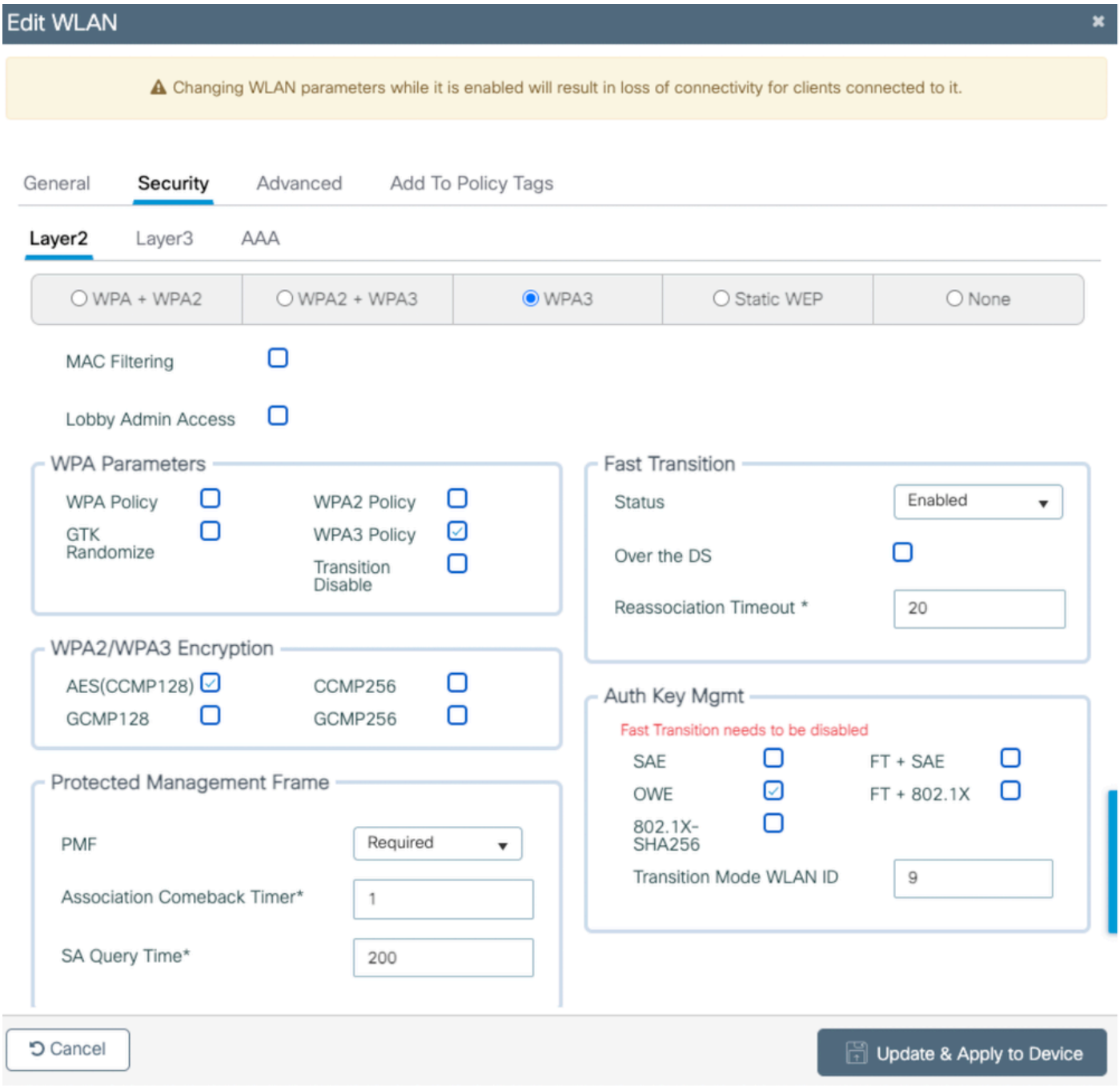

图9:在OWE转换SSID中启用FT时出现错误消息

PSK/dot1x不支持OWE

我们无法在这些组合中启用OWE，

1. 802.1x或FT+802.1x

2. PSK或FT+PSK或PSK-SHA256

3. SAE或FT+SAE

4. 802.1x-SHA256或FT+802.1x-SHA256

如果您尝试启用其中任何一种方法，则会收到错误消息，

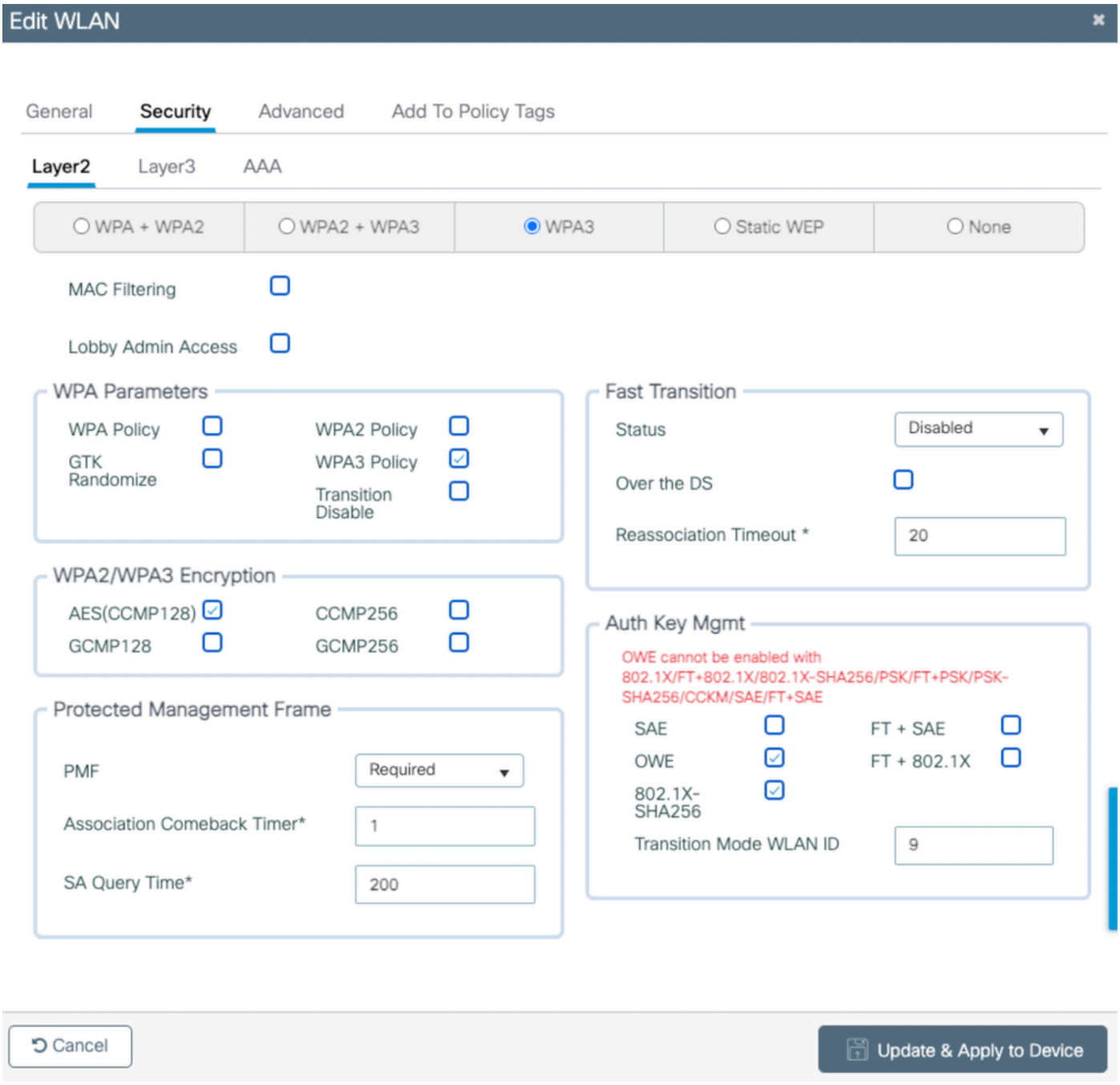

图10:在OWE SSID中启用其他身份验证方法时收到错误消息

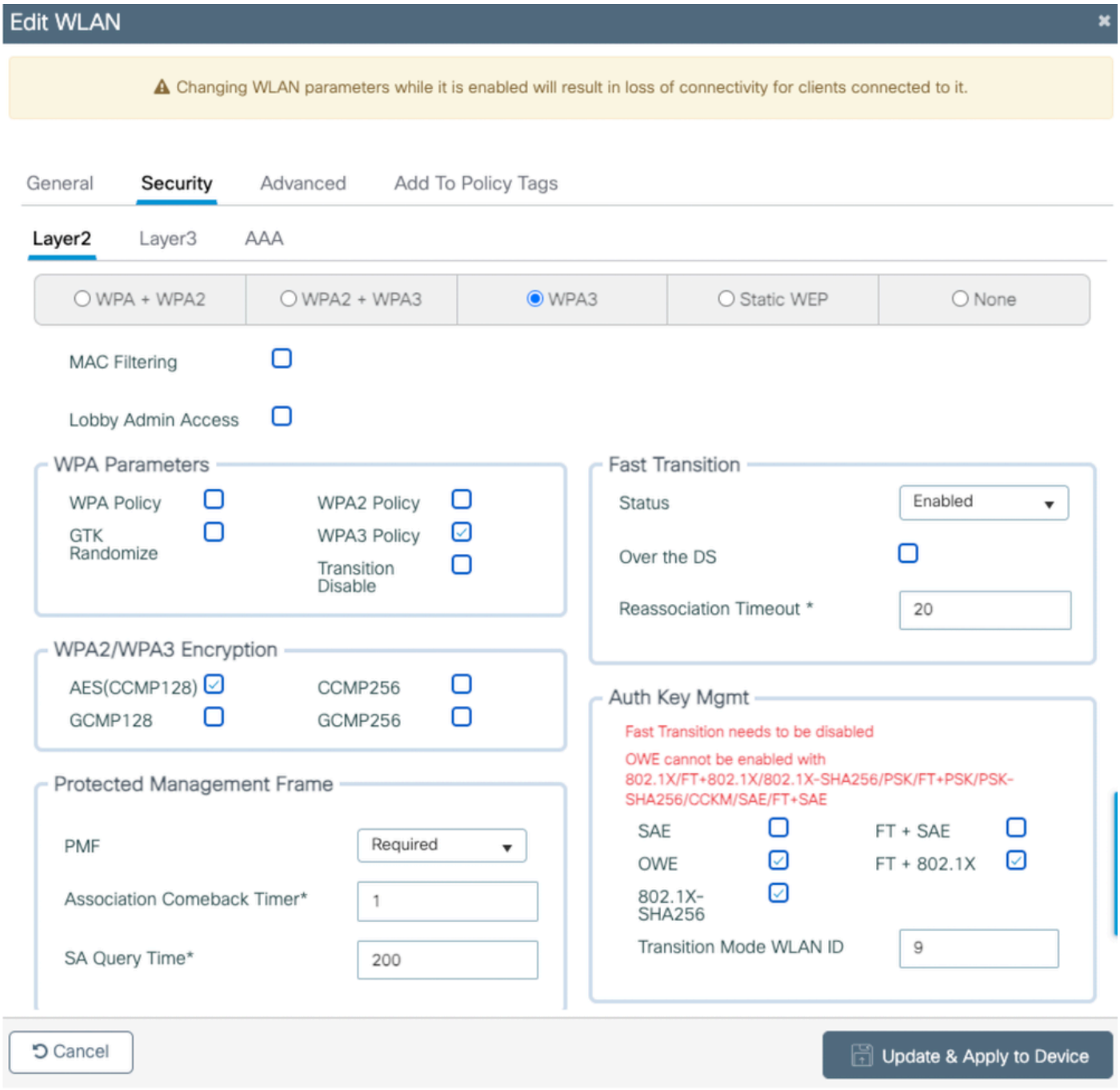

图11:启用AKM时出现错误消息

- 在Cisco IOS® XE 17.9.6 IOS版本中，当选择“WPA2+WPA3”时，您可以在AKM下看到“OWE”选项，但是您会收到错误消息，您不能将OWE与此组合一起使用。

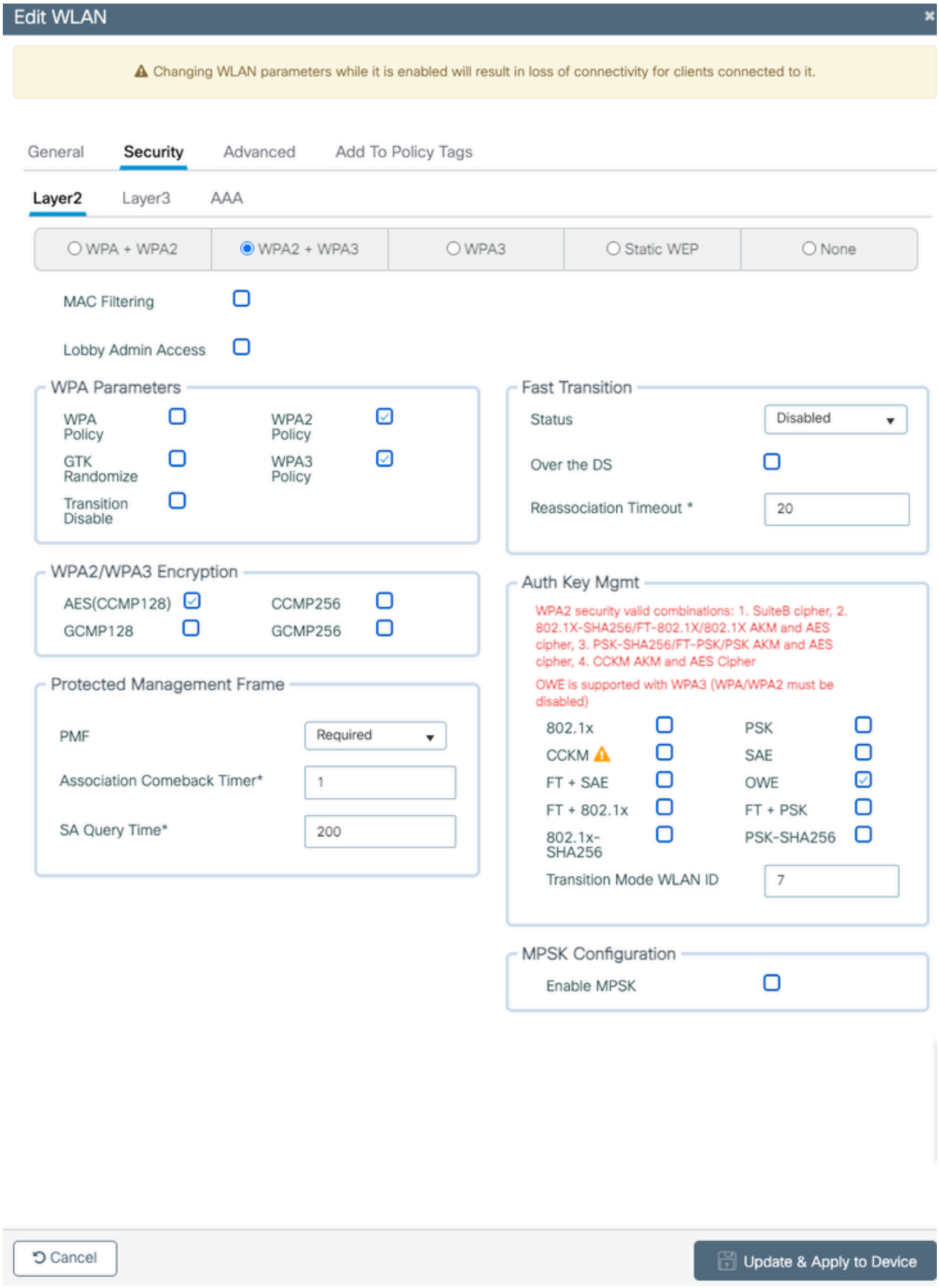

图12:选择WPA2+WPA3时出现错误消息

- 在Cisco IOS® XE 17.12.4版本中，当您选择“WPA2+WPA3”时，在AKM中无法获得“OWE”选

项，

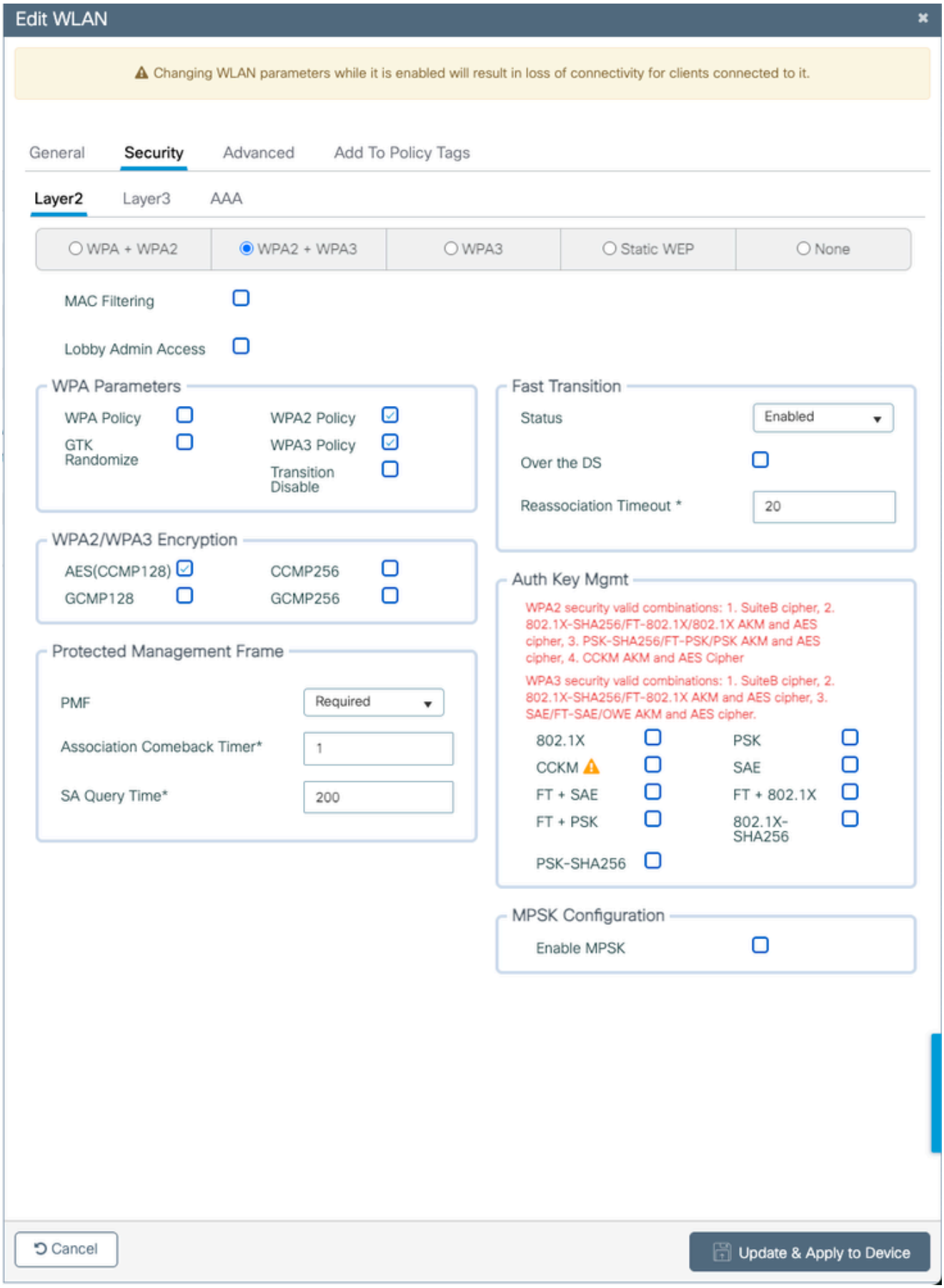

图13:错误消息 — 未获得AKM中的OWE选项

故障排除

1. 检查WLAN、OPEN SSID和OWE过渡SSID中的配置必须映射过渡WLAN ID。
2. 广播选项必须在OWE转换SSID中禁用，它只能在OPEN SSID中启用。
3. 检查本文中描述的支持的身份验证/加密/FT方法。
4. 如果WLC端的配置正常，请收集所需的日志和输出以缩小问题范围。

RA跟踪和EPC（嵌入式数据包捕获）

登录到WLC GUI -> Troubleshooting -> Radiative Trace -> Add client wifi MAC address -> Click that clients复选框 — > Start

登录到WLC GUI -> Troubleshooting -> Packet Capture -> Add new file name -> Choose the uplink interface and WMI VLAN/Interface -> Start。

从客户端计算机：如果可能，您可以通过选择WiFi接口安装Wireshark应用并收集数据包捕获。

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213949-wireless-debugging-and-log-collection-on.html#anc12

AIR PCAP

您可以通过使用MAC笔记本电脑或将AP之一配置为嗅探器模式来收集它，请参阅以下链接：

从MAC笔记本电脑：

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-mobility/217042-collect-packet-captures-over-the-air-on.html

从嗅探器AP:

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/217057-configure-access-point-in-sniffer-mode-o.html

将一台笔记本电脑（wireshark服务器）连接到交换机端口，其中必须安装wireshark应用程序，此wireshark服务器必须能够访问WLC WMI接口。如果协议“5555、5000或5556”出现在您的WLC和wireshark服务器之间，则需要在防火墙中允许该协议。

检查安装了wireshark的PC中是否安装了任何“gscaler”，如果不是，请“关闭”并尝试，如果是windows defender之类的防火墙或其中存在的任何内容，请禁用它们，然后尝试收集PCAP。

漫游

当客户端从一个AP漫游到另一个AP时，它需要执行以下步骤：

- 需要发送重新关联/关联 — 取决于客户端请求。
- 需要在关联请求中发送DH(Diffie-Helman)详细信息。

- 客户端可以从AP获取关联响应中的DH详细信息，基于此PMK在客户端和AP中生成。
- AP和客户端之间可以进行4次握手。
- 在OWE中，您无法启用FT，因此不可能使用802.11r。
- 每次客户端漫游时，需要在DH交换后进行关联四次握手。
- 客户端和AP使用自己的PMKID，对于每个AP和客户端来说都是唯一的。
- 如果客户端连接到同一个AP，则它可以使用同一个PMKID。在某些情况下，如果客户端被删除，比AP还多，则可以生成新的PMKID，但是客户端使用相同的PMKID进行4次握手。

示例：

如果客户端连接到同一个AP，则您可以在关联请求和关联响应中看到相同的PMKID。在关联响应中，如果DH使用同一PMKID，则无法查看DH详细信息。

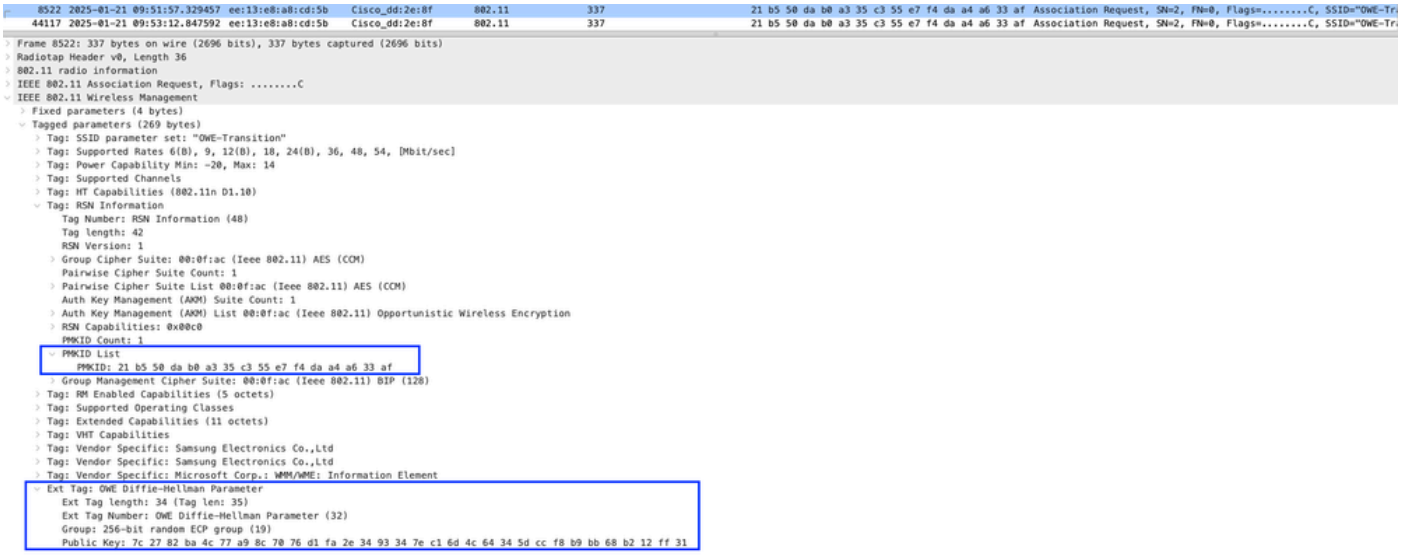

图14:使用同一PMKID

图15:与同一PMKID的关联响应

对于测试，从WLC手动删除此客户端，它再次关联到同一AP，此时，客户端发送同一PMKID，但AP在关联响应中发送DH详细信息。

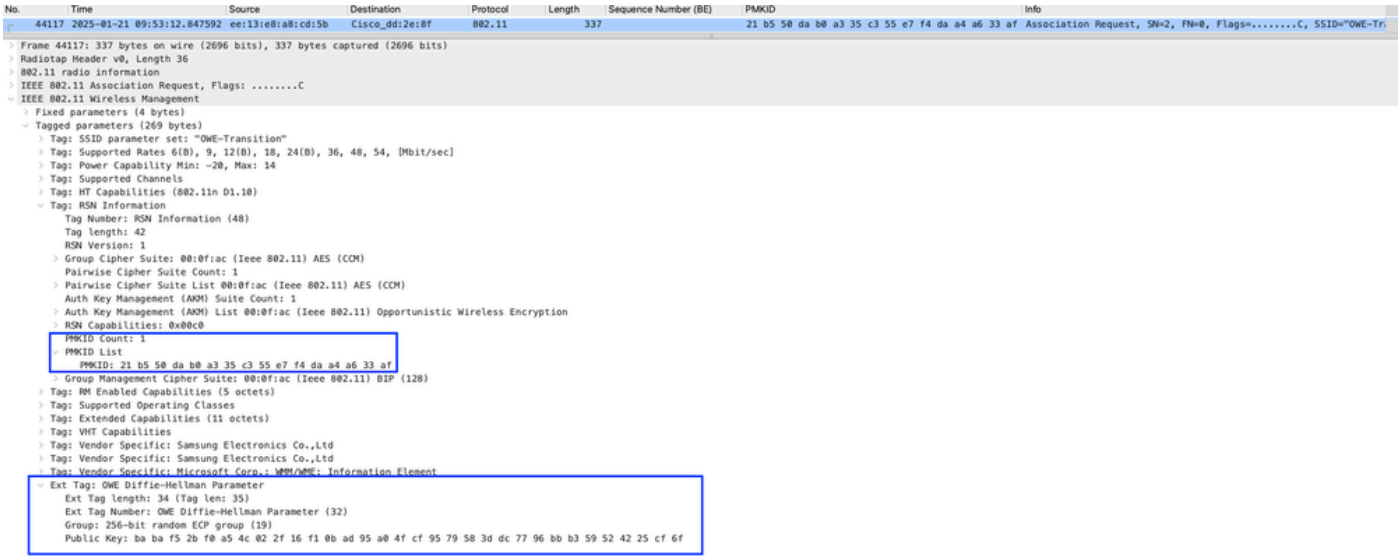

图16:删除后，客户端发送了包含DH详细信息的同一PMKID

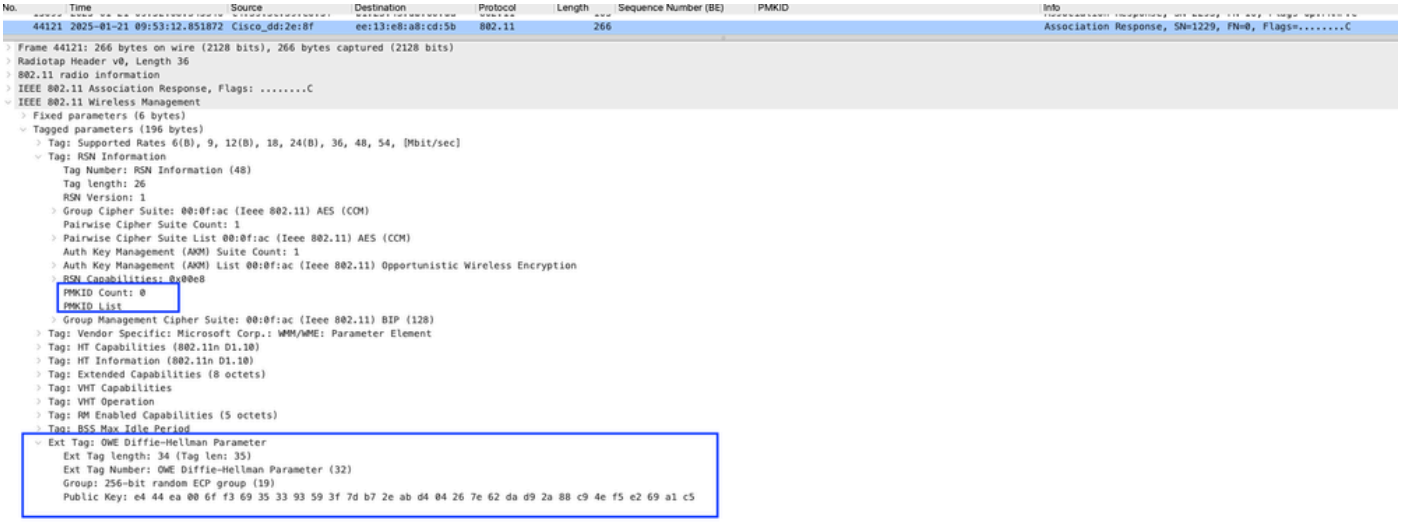

图17:AP使用DH值生成其新的PMKID

在本例中：AP和客户端在进行4次握手时使用同一个PMKID，请签入“M1和M2”消息。

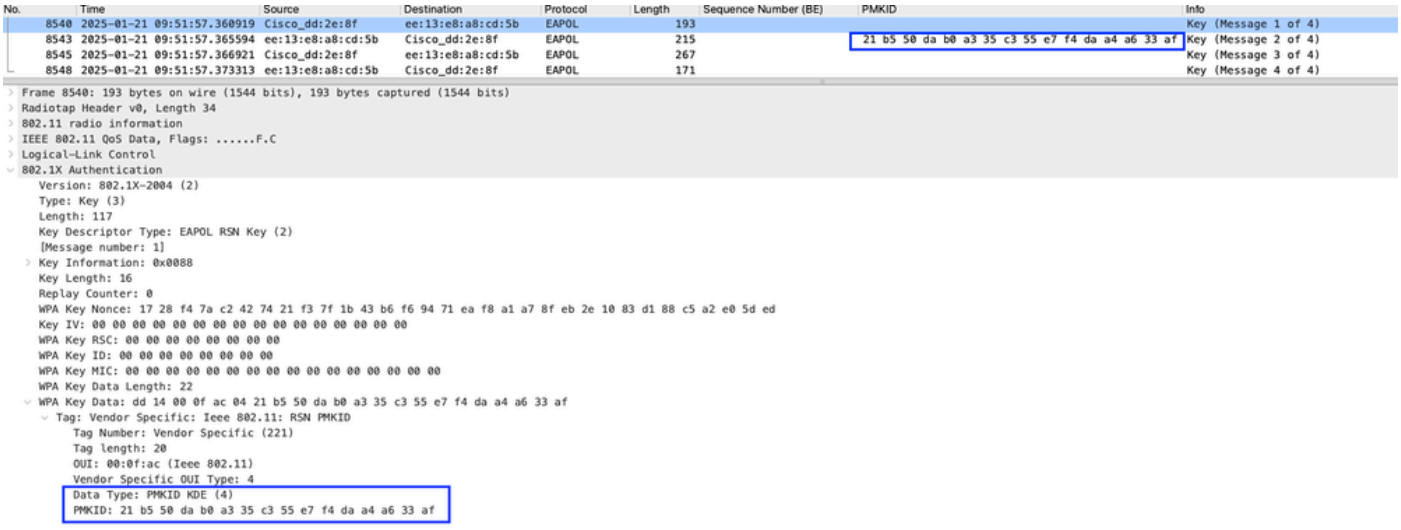

图 — 18:使用同一PMKID的AP和客户端

在本例中：客户端使用相同的PMKID，但AP使用在客户端被删除后生成的不同PMKID，请检查“M1和M2”消息。

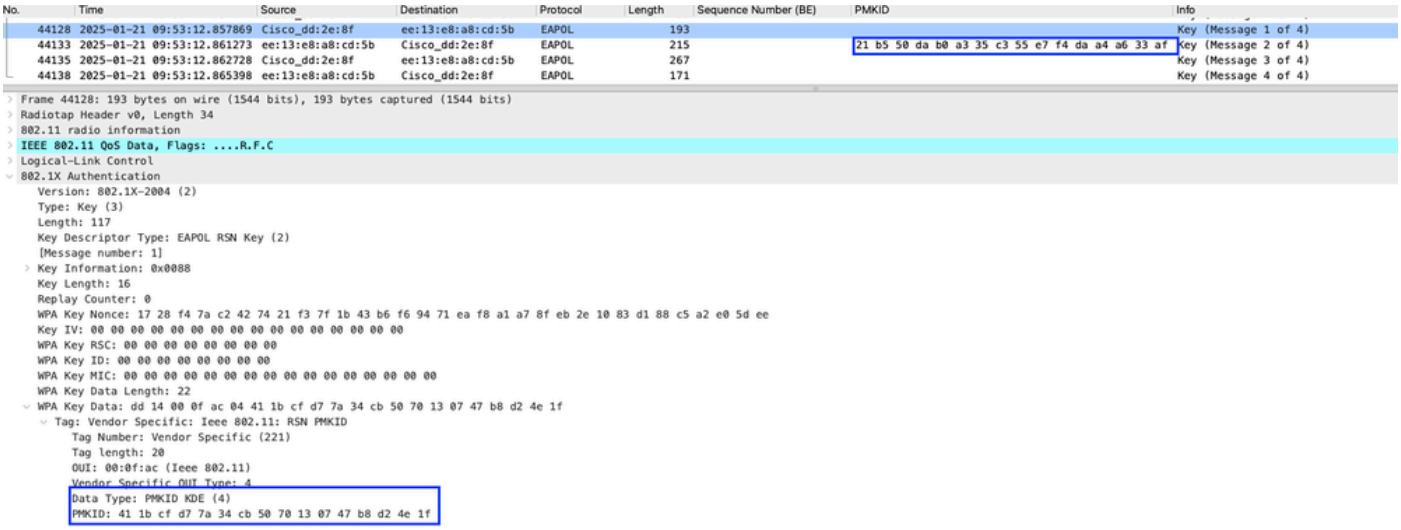

图19:使用不同PMKID的AP和客户端

从内部RA跟踪：

在本例中：客户端在关联请求和AP中发送的DH参数已处理，而不是生成PMK。

```
2025/01/21 15:18:50.157081690 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157082294 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157523328 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157531792 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157532236 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157532538 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157841380 {wncd_x_R0-0}{1}: [dot11-frame] [21675]: (debug): MAC: ee13.e8a8.cd5b  OW
```

此后，连接到同一AP的同一客户端，此时AP未生成新的PMKID，

```
2025/01/21 15:21:57.391898613 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391903915 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391906073 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391906329 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。